REMARKS

The Examiner has rejected Claims 1-36 under a double patenting rationale. This rejection is deemed avoided by virtue of the terminal disclaimer submitted herewith.

The Examiner has further rejected Claims 31-45 under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. Specifically, the Examiner asserts that the disclosure does not describe a computer program product embodied on a computer readable medium. Applicant respectfully disagrees. Note, for example, see Fig. 6 and the accompanying description for one non-limiting example of computer readable medium.

Claims 1-12, 16-27, and 31-42 stand rejected under 35 USC §103 as being unpatentable over Asai et al. (U.S. Patent 6,760,765) in view of Hailpern et al. (U.S. Patent 6,275,937). Applicant respectfully disagrees with such rejection, particularly in view of the amendment made hereinabove. Specifically, the subject matter of Claims 10, and 14-15 et al. has been incorporated into each of the independents claims.

With respect to the subject matter of former Claim 10 et al. (now incorporated into each of the independent claims), the Examiner, in a blanket manner, relies on col. 10, line 11 – col. 62 from Hailpern below to meet applicant's claimed technique "wherein said proxy devices are arranged to perform said malware scanning of files stored within the file storage device, and the load balancing device determines to which of said plurality of proxy devices to direct any particular access request; wherein each proxy device comprises: (a) a first interface for receiving from the load balancing device an access request issued by one of said client devices to said file storage device using the dedicated file access protocol; (b) a second interface for communicating with the file storage device to cause the file storage device to process the access request; (c) processing logic for causing selected malware scanning algorithms to be executed to determine whether the file identified by the access request is to be considered as malware" (see this or similar, but not necessarily identical language in each of the independent claims)

However, it appears that the Examiner has not taken into consideration the full weight of applicant's claims. First, after carefully reviewing the Hailpern except (and the entire reference, for that matter), there is simply not even suggest the specific selection of malware scanning algorithms, let alone processing logic in a plurality of proxy devices for accomplishing the same, as claimed. Still yet, Hailpern (and the remaining references, for that matter) fail to proxy devices, as claimed, which include two specific interfaces (in addition to the already-claimed client interface and proxy device interface), namely (a) a first interface for receiving from the load balancing device an access request issued by one of said client devices to said file storage device using the dedicated file access protocol, (b) a second interface for communicating with the file storage device to cause the file storage device to process the access request, as claimed.

Still yet, with respect to the subject matter of former Claims 14-15 et al. (now incorporated into each of the independent claims), the subject matter of such claim is rejected under 35 USC §103 as being unpatentable over Asai et al. (U.S. Patent 6,760,765) in view of Hailpern et al. (U.S. Patent 6,275,937), and further in view of Webb et al. (US 2002/00833342). Specifically, the Examiner relies on the excerpt from Webb below to meet applicant's claimed technique "wherein, upon receipt of an access request, the processing logic is arranged to determine from the access request predetermined attributes, and to send those predetermined attributes to the file storage device to enable the file storage device to perform a validation check, the processing logic only allowing the access request to proceed if the file storage device confirms that the client device is allowed to access the file identified by the file access request; wherein a user cache is utilized for storing the predetermined attributes" (see this or similar, but not necessarily identical language in each of the independent claims)

> "[0048] A Web page is served to the user's client that identifies each device on the private network for which the user has access rights (Block 240). According to alternative embodiments of the present invention, a secure cookie containing the user's log-in information and having a specified life span (e.g., 15 minutes after the last access) may be returned to the user's client with the served Web page (Block 245). The cookie may allow the user to

> access the Web server of any device that the user is authorized to access, but only for a specific time period. Each time the user accesses a device on the private network, the user's client sends the cookie to the gateway and the gateway determines whether the user is authorized to access the particular device. Upon expiration of the specified time period, the user would be required to log-in with the gateway. It is understood that embodiments of the present invention are not limited to the use of cookies. Alternatively, user log-in and/or session information may be encoded within a URL."

Again, it appears that the Examiner has not taken into consideration the full weight of applicant's claims. Specifically, the foregoing excerpt discloses that the gateway receives a cookie from a client and the gateway determines whether the user is authorized to access a particular device. Further, it appears that the Examiner assumes the following in Table 1.

Table 1

gateway = claimed "proxy"
cookie = claimed "attributes"
particular device = claimed "file storage device"

Assuming this, Webb still fails to meet applicant's claimed technique "wherein, upon receipt of an access request, the processing logic is arranged to determine from the access request predetermined attributes, and to send those predetermined attributes to the file storage device to enable the file storage device to perform a validation check, the processing logic only allowing the access request to proceed if the file storage device confirms that the client device is allowed to access the file identified by the file access request" (emphasis added). Only applicant teaches that the validation is performed by the file storage which, in turn, controls the proxy device in the manner claimed. Still yet, applicant also disagrees that the mere disclosure of a data structure such as a cookie meets applicant's claimed user cache utilized for storing the predetermined attributes.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or

in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck,*947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Applicant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above. A notice of allowance or a specific prior art showing of all of applicant's claim limitations, in combination with the remaining claim elements, is respectfully requested.

Finally, applicant disagrees with the Examiner's assertion that those limitations which were deemed "well known" under Official Notice previously are now admittedly common knowledge.

Thus, all of the independent claims are deemed allowable. Moreover, the remaining dependent claims are further deemed allowable, in view of their dependence on such independent claims.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. The Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAI1P476/01.124.01).

Respectfully submitted,
Zilka-Kotab, PC.

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100